UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

| | | |
|---|---|---|
| MALIBU MEDIA, LLC,<br><br>Plaintiff,<br><br>v.<br><br>JOHN DOE subscriber assigned IP address, 70.109.60.2,<br><br>Defendant. | ) | Civil Action No. 1:14cv1169 (TSE/JFA) |

**MEMORANDUM IN SUPPORT OF DEFENDANT'S MOTION FOR RECONSIDERATION AND TO QUASH THIRD-PARTY SUBPOENA**

Defendant JOHN DOE SUBSCRIBER ASSIGNED IP ADDRESS 70.109.60.2 ("John Doe"), by counsel, states the following in support of his Motion for Reconsideration of the Court's September 16, 2014 Order [Docket No. 6] and to Quash the third-party subpoena served by Plaintiff Malibu Media, LLC ("Malibu Media") on Verizon Online, LLC ("Verizon"):

**Introduction**

John Doe is a 60-year old resident of Virginia who, in September 2014, received a letter from Verizon, his Internet Service Provider (ISP), notifying him that he was the Verizon subscriber assigned IP address 70.109.60.2 at 5:43 UTC on August 21, 2014.[1] Copies of a third-party subpoena [attached hereto as Exhibit A] and Judge Anderson's September 16, 2014, Order authorizing the subpoena accompanied the Verizon letter.

[1] As discussed further herein, an IP address is not an "address" or physical "place" in the usual sense of the words, and therefore the term can be quite misleading. In fact, it is only an electronic "route" to the internet assigned by an ISP to a customer *at a given time* to provide access to the internet.

John Doe is one of thousands of "John Doe" defendants Malibu Media, a producer of online pornography, has sued throughout the United States alleging copyright infringement of its adult films. As of the date of this filing, PACER reflects that Malibu Media has commenced 2,963 actions in the federal courts, including nearly 100 cases in the Eastern District of Virginia in 2014 alone.

Malibu Media ostensibly uses the federal courts to enforce its copyrights against online infringement. Many have postulated that its court filings are a pressure tactic to drive rapid settlements from individuals humiliated by the threat of being associated with the viewing and distribution of pornographic films. Of the thousands of lawsuits Malibu Media has filed, it appears that only one has *ever* been taken to trial. Malibu Media's litigation tactics have garnered the attention of the Electronic Frontier Foundation ("EFF"), a digital rights watchdog, which describes the tactics succinctly in a backgrounder titled "*Malibu Media / EFF Calls for Court Sanctions For Copyright Troll's Public Humiliation Tactic*." As reported by the EFF,

> "[l]awyers representing the adult film producer Malibu Media, LLC file long lists of movie titles on the public record, accusing an Internet subscriber of copying those movies illegally. Among the titles on that list are many adult films with very embarrassing titles. The lawyers then send a copy of the court filing to the subscriber along with a demand for money. The threat is obvious – either pay up, point a finger at a friend or family member, or be named in a public lawsuit as a habitual user of hard-core porn. Faced with these threats, many people pay thousands to the lawyers to make the threat go away – whether they were responsible for illegal downloading or not. But more and more judges […] are catching on to copyright trolls' abuses of the justice system."

Article attached as Exhibit B, p.1.

The key to Malibu Media's litigation mill is its success in tagging the ISP subscriber identified with an IP address as the lawsuit's defendant. Malibu Media's cases are the digital equivalent of tagging a subdivision homeowner as the perpetrator of a theft committed on a

community walking path, with no factual support *whatsoever*, other than that the incident occurred on the portion of the path intersecting the homeowner's property.

It is exceedingly rare for a defendant to mount a defense against Malibu Media in court. The social stigma of being named by Malibu Media, and the high cost of litigation required to clear an innocent defendant's name, all but ensure a hasty settlement, however unfair to the defendant. Malibu Media's cases are reminiscent of those brought by another pornographer in this district, of which Judge Gibney stated:

> "[P]laintiffs have used the offices of the Court as an inexpensive means to gain the Doe defendants' personal information and coerce payment from them. The plaintiffs seemingly have no interest in actually litigating the cases, but rather simply have used the Court and its subpoena powers to obtain sufficient information to shake down the John Does."

15 K–Beech, Inc. v. John Does 1–85, Case No. 3:11-cv-469 (E.D. Va. 2011) (J. Gibney).

The continuing success of Malibu Media's tactics depends almost exclusively on acquiescence by the courts. Fortunately, more and more judges are becoming aware that the Malibu Media litigation machine is designed to extract payoffs without any evidence of misconduct. As discussed further herein, a number of federal courts have been willing, *sua sponte* or on motion, to reign in Malibu Media. John Doe respectfully requests that this Court do the same.

**Background on John Doe's Physical Address**[2]

According to Verizon, 70.109.60.2 was the IP address assigned to John Doe's subscriber account at 5:43 UTC on August 21, 2014. The internet service which Verizon provides to John Doe's account services a multi-residence, farmland property in Loudoun County, Virginia, by

[2] Endeavoring to avoid identifying John Doe, the undersigned counsel proffers the facts in this section. If the court desires direct testimony from John Doe confirming this proffer in order to decide this Motion, we ask to provide that testimony in a manner that avoids disclosure of John Doe's identity to Malibu Media.

means of an open (e.g. unsecured by any login/password protocol) wireless network. Internet service through this single subscriber account is accessible throughout the property, including at 11 distinct residences where approximately 30 different people, including John Doe, live on a permanent basis. Well over 100, and perhaps up to 200, guests have stayed overnight on the property in this year alone. The property is also serviced by employees and contractors. All of these people have had unrestricted access to the open wireless network.

Under a conservative estimate, 500 distinct devices are likely to have connected to the farm's wireless network in 2014. A great number of these connections resulted from numerous college students, who were guests on the property in January, May, and August of 2014 (the months in which Malibu Media claims its rights were infringed), using the network. John Doe does not know or control the content of electronic devices in the possession of other property residents, guests or contractors.

**Procedural Posture**

Malibu Media filed this action on September 8, 2014. Consistent with Malibu Media's practice of publically embarrassing its targets, the Complaint unnecessarily details the sexually explicit nature of Malibu Media's movies and includes an Exhibit that gratuitously-identifies pornographic film titles.

Malibu Media subsequently moved for leave to serve a non-party subpoena on Verizon, to discover the name, address, telephone number, and e-mail address of John Doe. The Court granted Malibu Media's motion for leave without a hearing or imposing any special conditions. Verizon is awaiting the resolution of today's Motion for Reconsideration and to Quash before disclosing John Doe's identity to Malibu Media.

## Legal Standard

Pursuant to Fed. R. Civ. P. 26(d)(1), absent a court order, a party may not propound discovery in advance of a Rule 26(f) conference. Rule 26(b) provides courts with the authority to authorize earlier discovery "for good cause[.]" The Court has plenary power to reconsider all interlocutory orders "as justice requires." Fayetteville Investors v. Commercial Builders, 936 F.2d 1462, 1473 (4th Cir. 1991). Pursuant to Rule 45(d)(3)(A)(iii), "[o]n timely motion, the court for the district where compliance [with a subpoena] is required must quash or modify a subpoena that […] requires the disclosure of privileged or other protected matter."

## Argument

### I. Many federal courts have *not* approved the early discovery tactic employed by Malibu Media here.

Plaintiff's Motion for Leave asserted that "Federal Circuit Courts have unanimously approved the procedure of suing John Doe defendants and then using discovery to identify such defendants." [Docket No. 4, p.5] This statement may conjure a false perception that Malibu Media's early discovery tactic has been universally accepted by the federal courts. That is decidedly not the case. Many federal courts have recognized that obtaining subscriber information for IP addresses is not a proper method for singling out a defendant for copyright infringement. Moreover, the circuit court cases cited by Plaintiff arose in wholly different contexts. The following representative cases, all involving online copyright infringement claims, demonstrate wide-spread *rejection* of what Malibu Media requested of this Court in its motion for leave to subpoena Verizon.

#### a. Illinois

In a similar case in which pornographers sought expedited discovery to learn the identity of persons "associated with" IP addresses, the court denied motions for expedited discovery and

reconsideration, noting that "IP subscribers are not necessarily copyright infringers […] The infringer might be the subscriber, someone in the subscriber's household, a visitor with her laptop, a neighbor, or someone parked on the street at any given moment." VPR Internationale v. Does 1-1017, No. 11-2068, 2011U.S. Dist. LEXIS 64656, at *3-4 (C.D. Ill. Apr. 29, 2011).

The risk of false identification by ISPs based on IP address is vividly illustrated in that same court order, by the court's retelling of a raid by federal agents on a home allegedly linked to downloaded child pornography. See id., at *3-4. The identity and location of the subscriber were provided by the ISP (in the same fashion that Malibu Media seeks to extract such information from Verizon.) See id. After the raid revealed no child pornography on the family computers (including iPhones and iPads), federal agents realized they had raided the wrong home. See id. The downloaded child pornography was later traced to a neighbor who had used multiple ISP subscribers' wireless internet connections. See id.

In Malibu Media v. Doe, No. 13-3694, 2013 U.S. Dist. LEXIS 78090 (N.D. Ill. June 3, 2013), the court acknowledged that "the increasing ubiquity of wireless networks undermines the copyright holder's assumption that the ISP subscriber is the copyright infringer." Id. at *2. Likewise, in cases TCYK, LLC v. Does 1-28, No. 13-3839, 2013 U.S. Dist. LEXIS 88401, at *6-7 (N.D. Ill. June 24, 2013) and TCYK, LLC v. Does 1-88, No. 13-3828, 2013 U.S. Dist. LEXIS 88402, at *6-7 (N.D. Ill. June 24, 2013), the court collected cases critical of naming ISP subscribers as presumed infringers.

**b. Florida**

A number of orders issuing in Malibu Media cases in the Southern District of Florida rejected Plaintiff's attempts to issue subpoenas for ISP subscriber identification. In Malibu Media v. Doe, 14-cv-20213 (S.D. Fla. March 20, 2014), the court issued a show cause order why

the court may reasonably rely on Malibu Media's usage of geolocation software[3] to establish the identity of a defendant. The judge was not satisfied with Malibu Media's explanations:

> "Plaintiff has not shown how this geolocation software can establish the identity of the Defendant. There is nothing that links the IP address location to the identity of the person actually downloading and viewing Plaintiff's videos[.] […] Even if this IP address is located within a residence, the geolocation software cannot identify who has access to that residence's computer and who would actually be using it to infringe Plaintiff's copyright. The Court finds that Plaintiff has not established good cause for the Court to reasonably rely on Plaintiff's use of geolocation to establish the identity of the Defendant."

Order attached hereto as Exhibit C, pp.1-2.

Likewise, in Malibu Media v. John Doe, 14-cv-20216, (S.D. Fla. February 10, 2014), the court found no "good cause" to deviate from Rule 26(d), denied early discovery and stated that "[t]he federal courts are not cogs in a plaintiff's copyright-enforcement business model." See Order attached as Exhibit D, pp.1-2. Later in the same case, upon a *sua sponte* review of the record, the court issued a show cause order regarding Malibu Media's reliance on geolocation to establish the identities of its defendants. See Order attached as Exhibit E. Malibu Media dropped the case.

**c. California**

In Discount Video Center, Inc. v. Does 1-5041, C 11-02694 (N.D. Cal. September 23, 2011), the Magistrate stated that he

> "has serious doubts as to the efficacy of the ISP subpoenas in uncovering the identity of the individuals alleged to have committed infringement. As the court has come to learn in yet another of the recent 'mass copyright' cases, subscriber information appears to be only the first step in the much longer, much more intrusive investigation required to uncover the identity of each Doe Defendant. The reason is simple: an IP address exposed by a wireless router might be used by the subscriber paying for the address, but

[3] Geolocation technology refers to services that purport to be able to identify the geographic location that an IP address is presently assigned to.

> it might not. Roommates, housemates, neighbors, visitors, employees or others less welcome might also use the same address."

Order attached as Exhibit F, p.3.

**d. New York**

The federal district courts in New York have also been reluctant to permit a subpoena to an ISP when confronted with a request similar to that made by Malibu Media. See, e.g., Patrick Collins, Inc. v. Doe 1, No. 12-cv-1154, 2012 U.S. Dist. LEXIS 165764, at *11-17 (E.D.N.Y. Nov. 20, 2012) (noting some courts' "skepticism of the use of IP addresses to identify file sharing defendants in cases involving pornographic films," and finding that an IP address alone is insufficient to establish a reasonable likelihood that it will lead to the identity of the defendants who could be sued). The preceding Report & Recommendation concluded

> "it is no more likely that the subscriber to an IP address carried out a particular computer function – here the purported illegal downloading of a single pornographic film – than to say an individual who pays the telephone bill made a specific telephone call. Indeed, due to the increasingly popularity of wireless routers, it is much less likely. While a decade ago, home wireless networks were nearly non-existent, 61% of US homes now have wireless access. […] As a result, a single IP address usually supports multiple computer devices – which unlike traditional telephones can be operated simultaneously by different individuals."

In Re: BitTorrent Adult Film Copyright Infringement Cases, 2012 U.S. Lexis 61447, at *9-10 (E.D.N.Y. May 1, 2012).

> "In sum, although the complaints state that IP addresses are assigned to 'devices' and thus by discovering the individual associated with that IP address will reveal 'defendants' true identity,' this is unlikely to be the case. Most, if not all, of the IP addresses will actually reflect a wireless router or other networking device, meaning that while the ISPs will provide the name of its subscriber, the alleged infringer could be the subscriber, a member of his or her family, an employee, invitee, neighbor, or interloper."

Id. at *13.

**e. Massachussetts**

In Combat Zone, Inc. v. Does 1-22, No. 12-30086, 2013 U.S. LEXIS 35429 (D. Mass Feb. 15, 2013), the court stated the following in connection with granting motions to quash: "The assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded a single sexually explicit film is tenuous, and one that has grown more so over time." Id. at *19 (internal citations omitted).

The obvious thread running through these cases is the court's unwillingness to authorize early, extraordinary discovery for the purpose of tagging an individual defendant based solely on an IP address. The factual contention that an IP subscriber is the infringer has no evidentiary support at the time of the Complaint, nor would it have evidentiary support even after the person's identity is disclosed. These courts were unwilling to be "cogs in a plaintiff's copyright-enforcement business model." Malibu Media v. John Doe, 14-cv-20216, (S.D. Fla. 2014) (Exhibit D, p.2).

## II. Dynamic IP addressing and the ease of IP spoofing further negate the subscriber-infringer link that Malibu Media urges on the Court.

Plaintiff's papers contend that "[t]he John Doe Defendant's IP address has been habitually used to infringe Plaintiff's copyrighted works." Malibu Media and its declarants deliberately omit discussion of the functionality of dynamic IP addressing. The Complaint's laundry list of film title "hits" covers many months. Dynamic IP addressing (including the standard DHCP protocol which Verizon FioS routers utilize), however, means that subscribers' IP addresses are not unique to them over time – they are subject to change and periodic reassignment to others. In other words, one Verizon subscriber, like John Doe, will have different IP addresses associated with his account over time.

At most, the current subpoena would identify the Verizon subscriber whose internet access was utilized, via IP address 70.109.60.2, on August 21, 2014 at 05:43:18 UTC. The personal information that Malibu Media would obtain would *not* be indicative of which Verizon subscriber account was assigned to IP address 70.109.60.2 on any of the 19 other 'Hit Dates' that Plaintiff deceptively strings together to create a specter of serial infringement by a single person.

Another inconvenient fact omitted from Malibu Media's papers is that, with modern Internet technology, virtually anyone can "spoof" an IP address. Spoofing is successfully masquerading a computer as a different computer. IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged IP address, with the purpose of concealing the identity of the sender or impersonating another computer. That is to say, one can spoof an IP address and make it appear that it was used to download a film from the BitTorrent Network, while the download was actually carried out by the hacker setting up the situation in a completely different location. The probative value of permitting Malibu Media to discover an ISP subscriber by IP address is therefore all the more lacking.

## III. Malibu Media's allegations are far thinner and more modest than they might have appeared to the court initially.

The Complaint alleges that Plaintiff's investigator, IPP International UG ("IPP"), "downloaded *from Defendant* one of [sic] more bits of each file has listed on Exhibit A. IPP further downloaded a full copy of each file hash *from the BitTorrent file distribution network*[.]"[4] Complaint ¶ 22 (emphasis added).

[4] The "BitTorrent file distribution network" reference indicates that IPP downloaded a copy of the allegedly infringed works – not from the IP address assigned to John Doe – but rather from other IP addresses in the far-flung peer-to-peer "swarm" network of BitTorrent users around the world.

Malibu Media does not allege that IPP detected a copy of even *one* of its films at the IP address associated with John Doe – rather its investigator merely downloaded "one of [sic] more bits" of information from the ID address associated with John Doe. Id. At least one federal court, the Central District of California, has stated that such an 'investigation' is unacceptable:

> "Plaintiffs did not conduct a sufficient investigation to determine whether that person actually downloaded enough data (or even anything at all) to produce a viewable video. Further, Plaintiffs cannot conclude whether that person spoofed the IP address, is the subscriber of that IP address, or is someone else using that subscriber's Internet access. Without better technology, prosecuting illegal BitTorrent activity requires substantial effort in order to make a case. It is simply not economically viable to properly prosecute the illegal download of a single copyrighted video. Enter Plaintiffs and their cottage-industry lawsuits."

Ingenuity 13 LLC v. Doe, 2:12-cv-8333 (C.D. Cal. May 6, 2013) (attached as Exhibit G, p.6).

In sum, Malibu Media's Motion for Leave persuaded the court to grant extraordinary discovery for Verizon to finger John Doe as a serial infringer of Malibu Media's works, based upon an agent's alleged downloading of as little as *one bit* of *one* allegedly protected work, at an appointed minute, on one day, when Verizon provided internet connectivity to the entire farm over an unsecured, distributed Wi-Fi network.

## IV. The incredibly tenuous nature of Plaintiff's claim and its scandalous allegations justify quashing the subpoena to protect John Doe's privacy interest.

Fed. R. Civ. P. 45 provides that a "court must quash or modify a subpoena that . . . requires disclosure of privileged or other protected matter . . . ." Rule 45(c)(3)(A)(iii). Under these circumstances, John Doe's identity is "privileged or other protected" information, and the Subpoena to Verizon should be quashed. Although John Doe's subscriber information might not have been protected in other circumstances, here, where there is no evidence whatsoever that implicates John Doe as an infringer, and where there is such a high risk of harm, John Doe has a legitimate expectation of privacy in his identity. Malibu Media should be precluded from further

harassing John Doe and trying to obtain information from Verizon that is not otherwise available to the public.

**Conclusion**

The ISP subscriber's name is simply not indicative of who improperly shared one "bit" of information, on one day, over an unsecured Wi-Fi network. No "good cause" warrants extraordinary discovery permitting Malibu Media to bootstrap a lawsuit and "discover" a defendant to sue on those facts. As numerous United States District Courts across the country have recognized in similar cases, a pornographer's desire to discover potential infringers of its copyrights doesn't justify *suing* any person they can place "on location" without more. At its heart, the expedited discovery sought here represented an effort by the Plaintiff to engage in *pre-suit discovery*, for the sole purpose of determining whether a cause of action exists and, if so, against whom the action should be instituted. This is not the proper purpose of a Rule 26(f) motion and is certainly not the intended use of a Rule 45 subpoena.

John Doe respectfully submits that the Court should not have granted the Plaintiff's extraordinary discovery request. Fortunately, this court has plenary power to reconsider its earlier order, and may also quash the outstanding subpoena to Verizon pursuant to Rule 45(c)(3)(A)(iii).

WHEREFORE, Defendant John Doe respectfully requests that the Court reconsider its earlier Order permitting Malibu Media to serve a third-party subpoena on Verizon, that the Court quash the outstanding subpoena, and grant such other relief as the Court deems just and proper.

Respectfully submitted,

/s/ Ryan C. Berry

Ryan C. Berry (Virginia Bar No. 67956)
Greenberg Traurig LLP
1750 Tysons Boulevard, Suite 1200
McLean, VA 22102
Telephone: 703.749.1369
Facsimile: 703.714.8388
berryr@gtlaw.com

*Counsel for Defendant*

**CERTIFICATE OF SERVICE**

I hereby certify that on the 30th day of October 2014, I caused the foregoing to be electronically filed with the Clerk of the Court using the CM/ECF system, which will then send a notification of such filing (NEF) to the following:

William Egbe Tabot, Esq.
William E. Tabot PC
9248 Mosby Street
Manassas, Virginia 20110-5038
703-530-7075
Fax: 703-530-9125
wetabotesq@wetlawfirm.com

*Counsel for Plaintiff*

/s/ Ryan C. Berry
Ryan C. Berry